PACIFIC TRIAL ATTORNEYS
A Professional Corporation
Scott J. Ferrell, Bar No. 202091
sferrell@pacifictrialattorneys.com
David W. Reid, Bar No. 267382
dreid@pacifictrialattorneys.com
Victoria C. Knowles, Bar No. 277231
vknowles@pacifictrialattorneys.com
4100 Newport Place Drive, Ste. 800
Newport Beach, CA 92660
Tel: (949) 706-6464
Fax: (949) 706-6469

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

REBEKA RODRIGUEZ,

Plaintiff,

v.

SIX FLAGS ENTERTAINMENT CORPORATION, a Delaware corporation, d/b/a WWW.KNOTTS.COM,

Defendant.

Case No. 2:25-cv-6661

COMPLAINT FOR VIOLATION OF THE FEDERAL WIRETAP ACT; THE CALIFORNIA INVASION OF PRIVACY ACT; AND RELATED COMMON LAW CLAIMS

I. INTRODUCTION

1. This case involves an outrageous privacy "bait and switch" scheme: Defendant lures visitors to its website at **knotts.com** (the Website) by assuring consumers that "[a]t Six Flags Entertainment Corporation … we take your privacy and the security of your information very seriously." *See* https://www.knotts.com/legal/privacy-policy (last accessed July 2025). In reality, Defendant secretly allows a notorious data broker to (1) intercept communications from visitors and (2) use those communications to compile and sell deeply personal details about visitors to the highest bidders. The predictable result is a grave intrusion upon visitor privacy.

2. The CEO of the world's largest data broker recently bragged about the suffocating extent to which data brokers secretly track internet users. Referring to a typical web user as "Lola," he boasts: "***We know who she is, what she watches, what she reads, and who she lives with. Through the power of connected identity, we also know who she follows on social media, what she buys online and offline, where she buys, when she buys, and more importantly, why she buys. We know that Lola has two children and that her kids drink lots of premium fruit juice. We can see that the price of the SKU she buys has been steadily rising on her local retailer's shelf. We can also see that Lola's income has not been keeping pace with inflation.***"[1]

3. Putting profits over privacy, has installed on its Website a spyware pixel called the "Claritas Tracking Pixel" to identify and spy on visitors to its website. Defendant secretly allowed Claritas to intercept the communication for the tortious purpose set forth below without Plaintiff's knowledge or consent (thus operating as a "Trap and Trace" device) to compile the dossiers described above and sell the information to the highest bidders. The conduct is outrageous and violates both federal and California law.

[1] Lucas Ropek, ***Data Broker Brags About Having Highly Detailed Personal Information on Nearly All Internet Users***, March 15 2025 (Gizmodo.com).

II. JURISDICTION AND VENUE

4. This Court has personal jurisdiction over Defendant because Defendant has sufficient minimum contacts with this District. Defendant's actions — installing tracking cookies and collecting data from a California resident—constitute purposeful direction toward California. Defendant's use of a tracking pixel with geolocation technology indicates awareness of California users' locations such that it has "expressly aimed" its conduct at California. There is a direct causal nexus between Defendant's conduct and Plaintiff's claims in that the unauthorized data collection and distribution were directly linked to Defendant's interactions with Plaintiff's device in California.

5. This Court has subject matter jurisdiction under 28 U.S.C. § 1331 because this action arises under 18 U.S.C. § 2510, *et seq.* (the Electronic Communications Privacy Act).

6. This Court has supplemental jurisdiction over the state law claims under 28 U.S.C. § 1367 because the state law claims form part of the same case or controversy under Article III of the United States Constitution.

7. Venue is proper in this District because a substantial part of the events or omissions giving rise to the claim occurred in this District.

III. PARTIES

8. Plaintiff is a resident and citizen of California.

9. Defendant is a North Carolina-based amusement park company that sells tickets to consumers nationwide via its Website. Defendant does business throughout the United States deriving substantial revenue from interstate commerce.

IV. FACTUAL ALLEGATIONS

A. Defendant Secretly Partners With A Data Broker To Intercept Visitor Communications And Sell Information About Their Private Lives To The Highest Bidders.

10. Defendant has installed on its Website a spyware pixel called "Claritas" to identify Website visitors (the "Claritas Spyware").

11. Claritas's spyware uses algorithms to analyze internet and device data and predict whether two or more devices are owned by the same person. Participating websites and apps then cater their advertisements based on a collective knowledge of the user's actions across all of their devices. Claritas uses data such as cookie IDs, operating system IDs, IP addresses, online registrations, and data from partnering publishers to develop a probability that different devices are shared by the same person.

12. Claritas is used for advertising to consumers across devices, where a user is shown an ad on their mobile or tablet device based on websites they visited on a desktop. For example, if an Android phone visits a website shortly after a desktop PC from the same home network, Claritas will assess that there is a high probability that the two devices are operated by the same person and will show them similar ads on both devices. Claritas also uses cross-device analytics for things like location, timing, user behavior, and audience analysis.

13. The Claritas Spyware activities described above are known as "fingerprinting." Put simply, the Claritas Spyware collects as much data as it can about an otherwise anonymous visitor to the Website and matches it with existing data Claritas has acquired and accumulated about hundreds of millions of Americans.

14. The Claritas Tracking Pixel is not merely an analytics tool — it is a powerful surveillance mechanism designed to identify and follow users across devices, sessions, and even websites, using a technique known as cross-device attribution. Here's how it works: **first**, when Plaintiff visited the Website, the Claritas Tracking Pixel was secretly loaded and covertly captured numerous device-specific attributes (including IP address, browser type and version, operating system, screen resolution, fonts and plugins, time zone, language, and hardware IDs). These data points were used to create a unique fingerprint of Plaintiff's device. **Second**, once Claritas collected this fingerprint and associated it with Plaintiff, it was able to link Plaintiff's activity across different devices (e.g., laptop → mobile phone), different browsers (e.g., Chrome → Safari), and different websites and sessions (e.g., visiting news site → shopping site) through both probabilistic

and deterministic methods. *See* https://claritas.com/multichannel-execution/ (describing use of cross-device attribution) (last downloaded July 2025). **Third**, the tracking was invisible to Plaintiff, as there was no visible indication that the tracking pixel was present and Plaintiff was not informed of the pixel or its purpose. **Fourth**, Defendant and Claritas collected and linked this cross-device data, and then sold it to third parties (advertisers, insurers, political campaigns, etc.), used to build consumer dossiers, including interests, income, health, and habits, and fed into real-time bidding systems to target users with tailored ads. *See* https://claritas.com/privacy-legal/ ("We share information with our business customers and other third parties for purposes of direct marketing (offline and online), advertising, and analytics services.") (last downloaded July 2025).

15. In short, the use of Claritas's Tracking Pixel on the Website is a surreptitious and invasive surveillance practice. Through cross-device attribution, it enables Claritas and its clients to secretly follow Plaintiff across Plaintiff's digital life without consent, visibility, or meaningful choice. In the context of privacy law, this practice is not only deceptive — it is profoundly intrusive and highly offensive to a reasonable person, especially when conducted under Defendant's false pretense to protect and respect Plaintiff's privacy, as described above.

16. Claritas is a data broker registered with the State of California Department of Justice. *See* https://oag.ca.gov/data-broker/registration/186480 (last accessed July 2025).

17. According to the esteemed Brennan Center for Justice, data brokers like Claritas are "the main purveyors of surveillance capitalism" that "collect, assemble, and analyze personal information to create detailed profiles of individuals, which they then sell to "financial institutions and insurance firms…Advertising companies… predatory loan companies, stalkers, and scammers…foreign actors…and law enforcement and other government agencies including the FBI and the IRS."). *See* https://www.brennancenter.org/our-work/research-reports/closing-data-broker-loophole (last accessed July 2025).

18. Plaintiff visited the Website in the last year to shop for amusement park tickets and was unaware of the secret spyware being used to surveil visitors and monetize their personal information. Plaintiff is both (1) genuinely interested in the goods, services, and information available on Defendant's Website, and (2) a consumer privacy advocate who works as a "tester" to ensure that companies abide by the privacy obligations imposed by California law. The Ninth Circuit recently made exceptionally clear that it is "necessary and desirable for committed individuals to bring serial litigation" to enforce and advance consumer protection statutes, and that Courts must not make any impermissible credibility or standing inferences against them. *Langer v. Kiser*, 57 F.4th 1085, 1095 (9th Cir. 2023).

19. The Claritas Spyware (1) begins to collect information the moment a user lands on the Website before any pop-up or cookie banner advises users of the invasion or seeks their consent; and (2) requests and transmits other identifying personal information to Claritas that allows Claritas to link a user's behavior on Defendant's website to the visitor's social media accounts.

B. The Claritas Tracking Pixel Spyware is a Trap and Trace Device.

20. Under the California Invasion of Privacy Act (CIPA), it is unlawful to use a "trap and trace" device without consent. The Claritas Tracking Pixel — when used to collect and transmit information about a website visitor's communications—falls squarely within the statutory definition of such a device.

21. CIPA § 638.50(c) defines a "trap and trace device" as: "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication."

22. CIPA makes it unlawful to install or use such a device without a court order or proper consent, even on a private communication system.

23. The Claritas Tracking Pixel is a "process" that captures routing and

addressing information. As shown above, it captures and transmits the IP address of the originating device, device identifiers such as cookies, device IDs, or browser fingerprints, URL referrer paths, headers, and session identifiers, and other dialing, routing, addressing, and signaling information that identifies the source of the user's electronic communication.

24. This data is the very type of "signaling information" contemplated by CIPA's definition of a trap and trace device. Just like a telephone trap and trace system captures the originating number, the Claritas Tracking Pixel identifies the originating digital sender — Plaintiff — through the routing and addressing metadata automatically included in the HTTP(S) request. The same principle applies here: the Claritas Tracking Pixel is a 21st century analog to a telephone trap and trace device—monitoring the metadata of electronic communications without consent.

25. Defendant did not obtain Plaintiff's express or implied consent to be subjected to fingerprinting and de-anonymization via the Claritas Tracking Pixel for the purposes of fingerprinting and de-anonymization, nor did Defendant obtain a Court order allowing it to install the Claritas Tracking Pixel.

26. CIPA imposes civil liability and statutory penalties for the installation of trap and trace software without a court order. Cal. P. Code § 637.2; s*ee also Shah v. Fandom, Inc*., No. 24-CV-01062-RFL, 2024 WL 4539577 (N.D. Cal. Oct. 21, 2024).

C. Defendant's Conduct is Highly Offensive To A Reasonable Person.

27. Defendant's "bait and switch" scheme – luring visitors to its Website by falsely promising that it will safeguard their privacy while secretly partnering with a notorious data broker to secretly track each visitor and sell their private information to the highest bidders – is highly offensive to a reasonable person for at least five reasons. **First**, it breaches trust and expectations – Defendant explicitly promised to protect Plaintiff's privacy, but secretly used the Claritas Tracking Pixel in direct contravention of its explicit assurances. **Second**, it involves deception because Defendant promises one thing but does the opposite. That kind of dishonesty makes the conduct more offensive

than ordinary tracking because it undermines autonomy and consent—cornerstones of digital privacy. **Third**, it occurs in a private and sensitive setting. **Fourth**, it enables unwanted third-party surveillance by allowing cross-site profiling and targeted advertising without Plaintiff's consent—something most people find invasive when done in secret. **Fifth**, it violates established privacy norms that companies will be transparent about tracking, obtain meaningful consent, and honor their privacy policies.

28. Defendant's conduct creates a genuine likelihood of serious harm to Plaintiff. The personal information Defendant surreptitiously harvested via the Claritas Tracking Pixel includes name, contact information, location data, browsing behavior, device fingerprints, and interests. This type of information can be — and has been — used for identity theft, targeted harassment, and manipulative advertising. Data brokers purchasing this information can assemble comprehensive profiles to discriminate, exploit, or endanger users, particularly vulnerable populations such as women, minors, and individuals seeking health services. The danger is not abstract: the FTC has warned that data sold to third parties may be used to expose sensitive locations like domestic violence shelters or reproductive clinics, as well as to facilitate stalking or physical tracking. Such practices impose serious privacy and safety risks, not mere discomfort.

29. Cross-device attribution is a technique used by data brokers and advertisers to link a person's activity across different devices — such as their phone, laptop, tablet, or smart TV. This means that even if someone switches from browsing on their phone to using a laptop, the data broker can still identify them as the same person.

30. Tracking pixels, which are tiny pieces of code embedded in websites or emails, are key to this. They quietly collect information like IP address, browser type, screen resolution, and behaviors like clicks or time spent on a page. When this data is combined with third-party data or identifiers (such as email hashes or cookies), it becomes possible to follow the user across multiple devices without their knowledge.

31. Lack of consent, visibility, or choice is a type of tracking that happens behind the scenes. Users aren't shown any clear notice that cross-device tracking is

happening. Often, even if privacy policies mention "personalized ads" or "analytics," they fail to disclose the true extent of this tracking, nor do they offer real choices (like opt-outs that actually work). That's why this practice has been criticized by regulators and privacy advocates as deceptive.

32. Courts and regulators (like the Federal Trade Commission and state Attorneys General) have increasingly recognized that undisclosed or misleading tracking practices — especially those that span across a person's devices and online life — are not just deceptive, but highly invasive.

33. This conduct is especially offensive when coupled with false privacy promises that Defendant will protect and respect user privacy. Courts have found that misleading consumers into thinking their privacy is respected — while secretly undermining that very privacy — is especially egregious and offensive.

34. The degree and setting of Defendant's intrusion is particularly severe – what sets Defendant's conduct apart is not just the nature of the information collected, but the context in which the intrusion occurred. The tracking took place in a purportedly trusted setting—Defendant's own corporate website—which explicitly assured Plaintiff that Plaintiff's privacy would be respected. Instead, Defendant implemented hidden surveillance code that began tracking Plaintiff without disclosure or authorization.

35. Defendant's motives and objectives were both deceptive and exploitative: the purpose of the intrusion further supports its offensiveness. Defendant did not track users for benign analytics or internal operations. Rather, Defendant partnered with a data broker known for trafficking in intimate and geolocation data—and did so to profit off of Plaintiff's personal information. This is not an isolated lapse in oversight; it is a deliberate business strategy premised on deception, surveillance, and commodification of user trust. Secretly surveilling users to profit from the sale of their personal data—while falsely promising not to—is the very definition of manipulative and predatory conduct.

36. There are no legitimate or countervailing interests or social norms that

render the intrusion inoffensive. **First**, the data at issue — such as real-time location, unique identifiers, or health-related browsing — is highly sensitive and context-dependent. **Second**, users cannot meaningfully consent to a practice they are never told about, especially when they are affirmatively misled. Moreover, there is no legitimate business or social interest in falsely promising privacy protections while secretly violating them. The only "interest" advanced by Defendant is financial profit derived from deception—an interest that cannot render the intrusion inoffensive under state and federal law.

37. The intrusion is "highly offensive." Taken together, the factors articulated by California courts—the severity of the intrusion, the deceptive setting, the potential for serious harm, the exploitative motive, and the lack of any countervailing justification—all weigh heavily in favor of a finding that the intrusion was highly offensive.

V. CAUSES OF ACTION

FIRST CAUSE OF ACTION

Violation of the Federal Wiretap Act

(18 U.S.C. § 2511)

38. The tracking pixel installed on Defendant's Website was used to intercept the contents of communications between Plaintiff and the Website in real time, including HTTP requests, URLs visited, and other metadata exchanged as part of Plaintiff's interactions with the site. These communications constitute "electronic communications" under 18 U.S.C. § 2510(12).

39. Defendant and/or its agents intentionally intercepted, or procured the interception of, these electronic communications using the tracking pixel technology, without Plaintiff's knowledge or consent.

40. The interception occurred contemporaneously with the transmission of the communication, satisfying the "in transit" requirement under the Wiretap Act.

41. No exception under 18 U.S.C. § 2511(2)(d) applies because Plaintiff did not consent to the interception, and Defendant exceeded any purported authorization by

misrepresenting the nature of the data collection and the identity of the third-party recipients.

42. Defendant acted with a tortious and unlawful purpose when it enabled and permitted a third-party data broker to intercept Plaintiff's electronic communications through the use of a tracking pixel embedded on Defendant website. Under 18 U.S.C. § 2511(2)(d), even if one party to a communication consents, the Wiretap Act is violated if the interception is made for the purpose of committing any criminal or tortious act. Courts have recognized that surreptitious data collection in violation of privacy rights can satisfy this "tortious purpose" standard. In *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589, 607 (9th Cir. 2020), the Ninth Circuit held that Facebook's interception of browsing activity via tracking technologies could constitute a violation of the Wiretap Act where the conduct was undertaken for the purpose of violating users' privacy rights, such as by committing the tort of intrusion upon seclusion. Here, Defendants' facilitation of a third-party's interception—despite promising to protect user privacy—was done with the purpose of enabling commercial exploitation of user data in violation of California common law privacy rights, including intrusion upon seclusion. This renders the interception unlawful under § 2511(2)(d).

43. As a result of this unlawful interception, Plaintiff is entitled to statutory damages under 18 U.S.C. § 2520, including the greater of actual damages or statutory damages of $100 per day per violation or $10,000, punitive damages, attorney's fees, and equitable relief.

SECOND CAUSE OF ACTION

Violations of the California Trap and Trace Law

Cal. Penal Code § 638.51

44. California's Trap and Trace Law is part of the California Invasion of Privacy Act ("CIPA") codified at Cal. Penal Code 630, *et. seq*.

45. CIPA was enacted to curb "the invasion of privacy resulting from the continual and increasing use of" certain technologies determined to pose "a serious threat

to the free exercise of personal liberties." CIPA extends civil liability for various means of surveillance using technology, including the installation of a trap and trace device.

46. A "trap and trace device" as "a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication." Cal. Penal Code § 638.50(c).

47. California Penal Code § 638.51(a) provides that "a person may not install or use…a trap and trace device without first obtaining a court order…."

48. Defendant uses a trap and trace process on its Website by deploying the Claritas Tracking Pixel Spyware on its Website because it captures routing, addressing and/or other signaling information of website visitors including Plaintiff.

49. Defendant did not obtain consent from Plaintiff before using trap and trace technology to identify users of its Website and has violated section 638.51 and did not obtain a court order to do so.

50. CIPA imposes civil liability and statutory penalties for violations of section 638.51. Cal. Penal Code § 637.2.

THIRD CAUSE OF ACTION

California Intrusion Upon Seclusion

51. Defendant intentionally intruded upon the private affairs, concerns, and seclusion of Plaintiff by improperly accessing Plaintiff's personal information and using it for improper purposes, including by partnering with a data broker to sell Plaintiff's private information to the highest bidder and by targeting Plaintiff with behavioral advertising.

52. Defendant's intrusions upon the private affairs, concerns, and seclusion of Plaintiff has been substantial and would be highly offensive to a reasonable person and constitute an egregious breach of social norms, as is evidenced by countless consumer surveys, studies, and op-eds decrying the online tracking of website visitors, centuries of

common law, state and federal statutes and regulations, legislative commentaries, enforcement actions undertaken by the FTC, industry standards and guidelines, scholarly literature on consumers' reasonable expectations, and the penalties imposed by the FTC and other regulatory bodies.

53. Plaintiff did not consent to Defendant's intrusions. Indeed, as shown above, Defendant promised that it would protect Plaintiff's privacy.

PRAYER

WHEREFORE, Plaintiff prays for the following relief against Defendant:

1. Actual and statutory damages;
2. Reasonable attorneys' fees and costs;
3. An injunction to prevent the unlawful conduct alleged above; and
4. All other relief that would be just and proper as a matter of law or equity, as determined by the Court.

Dated: July 22, 2025

PACIFIC TRIAL ATTORNEYS, APC

By: _____
Scott. J. Ferrell
Attorneys for Plaintiff